UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/901,286	07/09/2001	Hal Joseph Burch	2-9	7595

7590 03/21/2006

Lucent Technologies Inc.
Docket Administrator (Room 3J-219)
101 Crawfords Corner Road
Holmdel, NJ 07733

EXAMINER	
HOFFMAN, BRANDON S	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 03/21/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/901,286	BURCH ET AL.	
	Examiner	Art Unit	
	Brandon S. Hoffman	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *07 December 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-30* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-30* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-30 are pending in this office action.

2. Applicant's arguments, filed December 7, 2005, have been fully considered but they are not persuasive.

Rejections

3. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Claim Rejections - 35 USC § 103

4. Claims 1-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gupta et al. (U.S. Patent No. 6,658,565) in view of Munger et al. (U.S. Patent No. 6,502,135).

Regarding claims 1 and 16: Gupta et al. discloses a method/apparatus for tracing a sequence of packets to a potential source thereof within a communications network, the sequence of packets being received at a target host in said communications network at a received packet rate, the method comprising the steps of:

- For each selected network element, measuring a change in said received packet rate in response to said application of said burst load to said selected network element (col. 7, line 66 through col. 8, line 2); and
- Determining said potential source of said sequence of packets based on said measured changes in said received packet rate (col. 8, lines 2-4).

Gupta et al. does not teach applying a burst load to each of one or more selected network elements in said communications network.

Munger et al. teaches applying a burst load to each of one or more selected network elements in said communications network (col. 10, lines 6-21).

It would have been obvious to one of ordinary skill in the art, at the time the invention was made, to combine applying burst loads to each network element, as taught by Munger et al., with the method/apparatus of Gupta et al. It would have been obvious for such modifications because bursts of packets on a network element can help determine the identities of the sender and receiver (see col. 2, lines 49-51 of Munger et al.).

Regarding claims 2 and 17: Gupta et al. as modified by Munger et al. discloses wherein said communications network comprises the Internet (see col. 2, lines 51-56 of Gupta et al.).

Regarding claims 3 and 18: Gupta et al. as modified by Munger et al. discloses wherein each of said selected network elements comprises a network link (see fig. 2, ref. num 208 of Gupta et al.).

Regarding claims 4 and 19: Gupta et al. as modified by Munger et al. discloses wherein said step of applying a burst load to said network link comprises transmitting packets to a sub network of said communications network to initiate a responsive flow of packets through said network link (see col. 4, lines 35-42 of Munger et al.).

Regarding claim 5 and 20: Gupta et al. as modified by Munger et al. discloses wherein said transmitted packets are spoofed from an end of said network link closest to said target host (see col. 3, lines 42-48 of Gupta et al., DoS attacks are performed by spoofing the source address).

Regarding claims 6 and 21: Gupta et al. as modified by Munger et al. discloses wherein said transmitted packets comprise UDP chargen requests (see col. 9, lines 64-65 of Munger et al.).

Regarding claims 7 and 22: Gupta et al. as modified by Munger et al. discloses wherein each of said selected network elements comprises a network router (see col. 1, line 25 of Gupta et al.).

Regarding claims 8 and 23: Gupta et al. as modified by Munger et al. discloses further comprising the step of generating a map comprising routes from said target host to a plurality of sub networks of said communications network (see col. 1, line 25, a router is known to have a routing table of all sub network elements connected to it).

Regarding claims 9 and 24: Gupta et al. as modified by Munger et al. discloses further comprising the step of eliminating said selected network element from consideration as said potential source of said sequence of packets when said change in said received packet rate meets a predetermined criterion (see col. 7, line 66 through col. 8, line 6 of Gupta et al.).

Regarding claims 10 and 25: Gupta et al. as modified by Munger et al. discloses wherein said predetermined criterion comprises a determination of whether said change in said received packet rate is less than a predetermined threshold (see col. 8, lines 2-6 of Gupta et al.).

Regarding claims 11 and 26: Gupta et al. as modified by Munger et al. discloses wherein said step of eliminating said selected network element from consideration also eliminates from consideration one or more sub networks of said communications network which are connected to said selected network element (see col. 8, lines 2-6 of Gupta et al., sub networks, which are connected to the parent network element, would

inherently be eliminated from suspicion because of their dependency on the parent network element).

Regarding claims 12 and 27: Gupta et al. as modified by Munger et al. discloses wherein said sequence of packets comprises a Denial-of-Service attack on said target host (see abstract of Munger et al.).

Regarding claims 13 and 28: Gupta et al. as modified by Munger et al. discloses wherein said steps of applying said burst load, measuring said changes in said received packet rate, and determining said potential source of said sequence of packets, are executed under the control of an automated algorithm (see col. 7, lines 60-62 of Gupta et al.).

Regarding claims 14 and 29: Gupta et al. as modified by Munger et al. discloses wherein said steps of applying said burst load and determining said potential source of said sequence of packets, are executed under the at least partial control of a human operator (see col. 7, lines 50-52 and 63-66 of Gupta et al.).

Regarding claims 15 and 30: Gupta et al. as modified by Munger et al. discloses further comprising the step of displaying information, said information including data representative of said measured changes in said received packet rate, to said human operator, for use by said human operator in exercising said at least partial control (see

col. 7, lines 50-52 and 63-66 of Gupta et al., GUI's are commonly used to change settings).

Response to Arguments

5. Applicant argues:

a) Gupta et al. does not teach tracing a sequence of packets to a potential source (page 3, second paragraph).

b) Gupta et al. does not teach measuring a change in said received packet rate in response to said application of said burst load (page 3, third paragraph).

c) Gupta et al. does not teach determining a potential source of a sequence of packets (page 3, last paragraph through page 4, first paragraph).

d) Munger et al. does not teach applying a burst load to each of one or more selected network elements (page 4, second paragraph).

Regarding argument (a), examiner disagrees with applicant. In response to applicant's arguments, the recitation "*tracing a sequence of packets to a potential source*" has not been given patentable weight because the recitation occurs in the preamble. A preamble is generally not accorded any patentable weight where it merely recites the purpose of a process or the intended use of a structure, and where the body of the claim does not depend on the preamble for completeness but, instead, the process steps or structural limitations are able to stand alone. See *In re Hirao*, 535

F.2d 67, 190 USPQ 15 (CCPA 1976) and *Kropa v. Robie*, 187 F.2d 150, 152, 88 USPQ 478, 481 (CCPA 1951).

Regarding argument (b), examiner disagrees with applicant. Gupta et al. measures and detects a change in rate of the received packet rate in order to determine if a network attack is taking place (col. 7, line 66 through col. 8, line 2). The citation of Gupta et al. teaches that, in response to an increased load on the network (a burst), the switch determines that an intrusion is taking place. This shows the measuring a rate change in response to an applied burst.

Regarding argument (c), examiner disagrees with applicant. Column 1, lines 45-60 of Gupta et al., shows that the switch monitors/records all frame traffic... that are transmitted from a particular sender... to ensure the sender does not exceed a threshold. This monitoring of a particular sender would have to know the source of the frame traffic, as identified in the frame traffic (see fig. 4, ref. num 410 of Gupta et al.).

Regarding argument (d), examiner disagrees with applicant. In addition to Gupta et al. teaching monitoring a burst load on a network to determine an intrusion, column 2, lines 37-51 of Munger et al., shows that bursts of packets from a user during low-duty periods can reveal the identities of sender and receiver. The cited portion of Munger et al. (col. 10, lines 6-21), says that dummy data or decoy data can be added as an option. It is not required. Munger et al. understands that burst loads can be used for identifying the source and destination of packets. The claim calls for applying burst loads to each of one or more selected network elements.

Conclusion

6. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon S. Hoffman whose telephone number is 571-272-3863. The examiner can normally be reached on M-F 8:30 - 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Brenda Hall

BH

CHRISTOPHER REVAK
PRIMARY EXAMINER

Cel 3/17/06